### U.S. Serial Number 09/734,809 Atty. Docket # AUS9-2000-0799-US1 Benantar

Method and system for a secure binding of a revoked X.509 certificate to its corresponding certificate revocation list

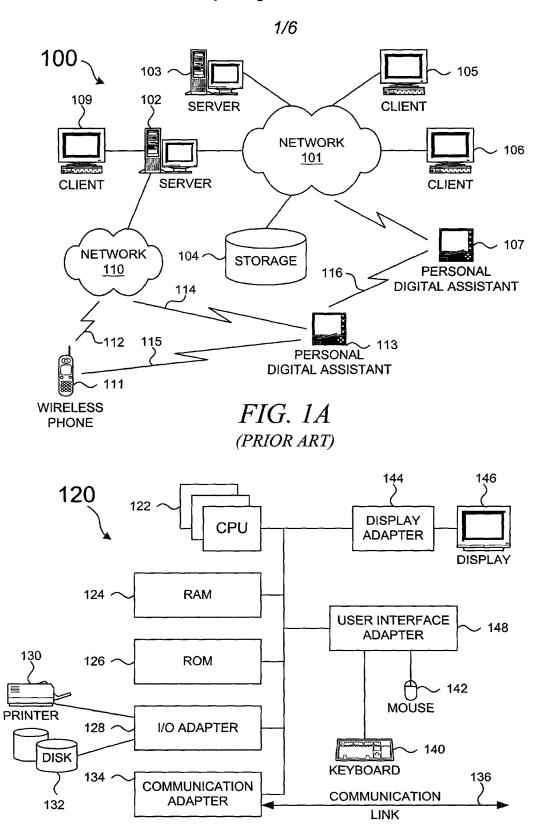


FIG. 1B (PRIOR ART)

# U.S. Serial Number 09/734,809 Atty. Docket # AUS9-2000-0799-US1 Benantar

Method and system for a secure binding of a revoked X.509 certificate to its corresponding certificate revocation list



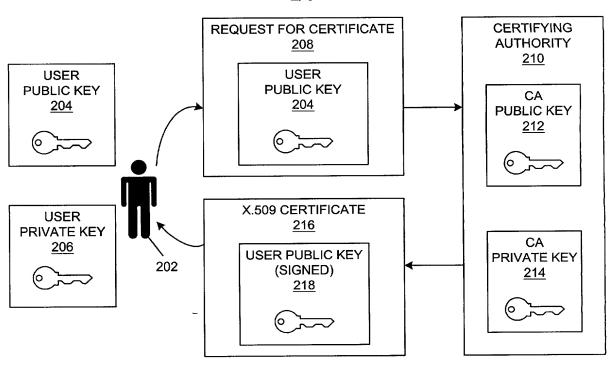


FIG. 2 (PRIOR ART)

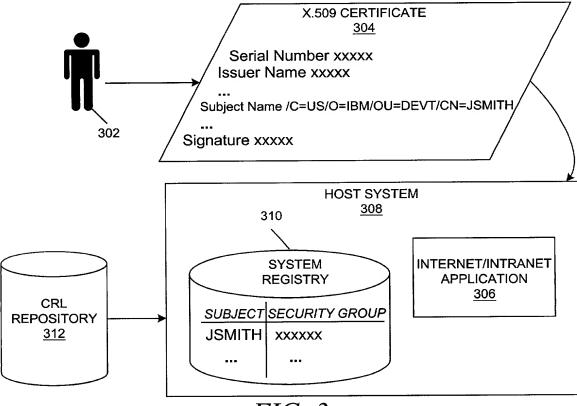


FIG. 3
(PRIOR ART)

# U.S. Serial Number 09/734,809 Atty. Docket # AUS9-2000-0799-US1 Benantar

Method and system for a secure binding of a revoked X.509 certificate to its corresponding certificate revocation list

3/6

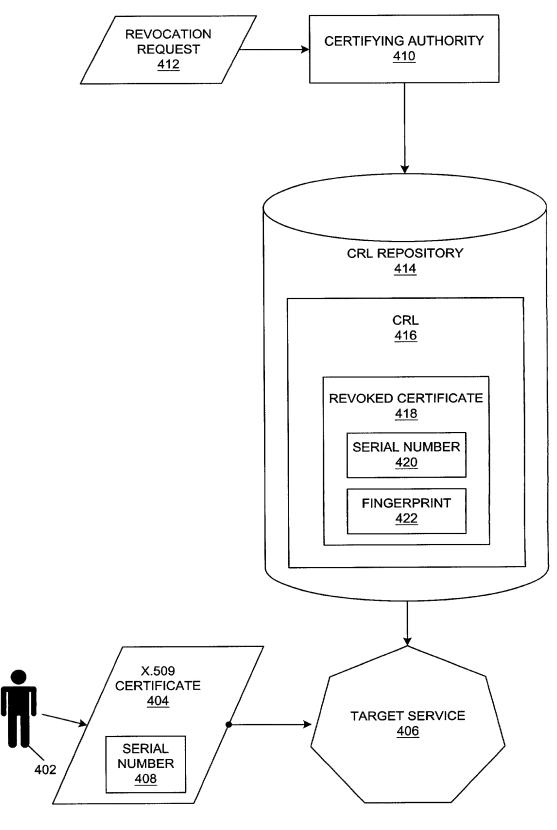


FIG. 4

### U.S. Serial Number 09/734,809 Atty. Docket # AUS9-2000-0799-US1 Benantar

# Method and system for a secure binding of a revoked X.509 certificate to its corresponding certificate revocation list

4/6

```
Certificate ::= SEQUENCE
      tbsCertificate
                              TBSCertificate,
                              AlgorithmIdentifier,
      signatureAlgorithm
      signature
                              BIT STRING }
                     SEQUENCE {
TBSCertificate ::=
                        [0]
                              Version DEFAULT v1,
      version
      serialNumber
                              CertificateSerialNumber,
                              AlgorithmIdentifier,
      signature
      issuer
                              Name,
      validity
                              Validity,
      subject
                              Name,
      subjectPublicKeyInfo
                              SubjectPublicKeyInfo,
                              IMPLICIT UniqueIdentifier OPTIONAL,
      issuerUniqueID
                        [1]
                              IMPLICIT UniqueIdentifier OPTIONAL,
      subjectUniqueID
                        [2]
      extensions
                        [3]
                              Extensions OPTIONAL
Version ::= INTEGER \{ v1(0), v2(1), v3(2) \}
CertificateSerialNumber
                        ::= INTEGER
Validity ::= SEQUENCE {
     notBefore
                              Time,
     notAfter
                              Time }
Time ::= CHOICE {
                              UTCTime,
      utcTime
      generalTime
                              GeneralizedTime }
UniqueIdentifier ::= BIT STRING
SubjectPublicKeyInfo
                           SEQUENCE {
                     ::=
      algorithm
                              AlgorithmIdentifier,
      subjectPublicKey
                              BIT STRING }
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE
                              OBJECT IDENTIFIER,
      extnID
      critical
                              BOOLEAN DEFAULT FALSE,
                              OCTET STRING }
      extnValue
```

FIG. 5A (PRIOR ART)

# h is a complete to the property of

## U.S. Serial Number 09/734,809 Atty. Docket # AUS9-2000-0799-US1 Benantar

# Method and system for a secure binding of a revoked X.509 certificate to its corresponding certificate revocation list

5/6

```
CertificateList ::= SEQUENCE {
       tbsCertList
                             TBSCertList,
       signatureAlgorithm
                             AlgorithmIdentifier,
       signatureValue
                             BIT STRING }
TBSCertList ::= SEQUENCE {
       version
                             Version OPTIONAL,
       signature
                             Algorithmidentifier,
       issuer
                             Name,
       thisUpdate
                             Time,
                             Time OPTIONAL,
       nextUpdate
       revokedCertificates
                             SEQUENCE OF SEQUENCE {
              userCertificate
                                     CertificateSerialNumber,
              revocationDate
                                     Time.
              crlEntryExtensions
                                    Extensions OPTIONAL
       } OPTIONAL,
                             EXPLICIT Extensions OPTIONAL
       crlExtensions
                     [0]
}
                                     FIG. 5B
                                     (PRIOR ART)
certFingerprint ::= SEQUENCE OF SEQUENCE {
                             AlgorithmIdentifier,
       algorithm
       fingerprint
                             octet string
}
```

FIG. 6

### U.S. Serial Number 09/734,809 Atty. Docket # AUS9-2000-0799-US1 Benantar

Method and system for a secure binding of a revoked X.509 certificate to its corresponding certificate revocation list

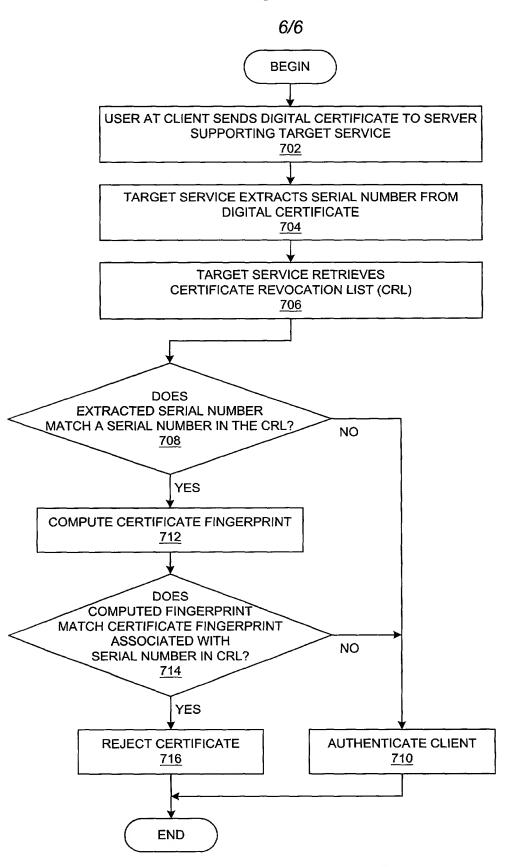


FIG. 7